Quick Guide to HIPAA Security Compliance

This Security Standards Matrix is Appendix A to Subpart C of Part 164 in the final HIPAA Security Rule. The matrix contains a listing of the security standards as well as where each of the standards and implementation specifications can be found in the security rule.

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a) (2)	(R)
Workforce Security	164.308(a) (3)	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)
Information Access Management	164.308(a) (4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a) (5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a) (6)	Response and Reporting (R)
Contingency Plan	164.308(a) (7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a) (8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b) (1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a) (1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d) (1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards		
Access Control	164.312(a) (1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c) (1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

T R I C A R E

TRICARE MANAGEMENT ACTIVITY